Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Improving 9-1-1 Reliability	)	PS Docket No. 13-75
	)	
Reliability and Continuity of Communications	)	
Networks, Including Broadband Technologies	)	PS Docket No. 11-60

COMMENTS

To: The Commission

The Information Technology Advisory Commission of Arlington County, Virginia ("Arlington ITAC") hereby submits its Comments in the above captioned proceeding.

The U.S. has made significant efforts in the past decade to catch up with other leading countries in terms of broadband communications, implementation of fiber optics and gigabit satellite systems, expanded use of Voice over IP ("VOIP"), and most recently fourth generation LTE wireless communication systems. In seeking to implement truly high-speed fiber and wireless systems, however, there is a danger that various vulnerabilities associated with these new systems may be left exposed to cyber-attack or other serious risk factors. These potential or even quite dangerous vulnerabilities may have been overlooked in the rush to upgrade and modernize IT and telecommunications networks. Beyond the architecture and operating systems for these new broadband networks there are also issues related to power systems and SCADA systems and how their reliable operation can be protected from cyber attack or from interruption due to industrial accident or natural catastrophe.

Arlington ITAC, , with information from Staff of the Arlington County Department of Technology Services and national and international experts in the field of disaster management and security enhancement, has discovered a number of security concerns and risk factors that we feel are crucial for the Federal Communications Commission ("FCC") to address in its current inquiries. We do not claim to have the best or most cost effective solution to these security concerns, but feel we serve the public interest by highlighting them to the FCC and the Department of Homeland Security ("DHS") through this filing. We believe that specific corrective regulatory measures, new legislation, or at least wide-spread voluntary corporate "Best Practices" should be adopted to address these concerns and vulnerabilities.

Emergency, Governmental, Business and Consumer Telecommunications During Power Outages: During the violent Derecho storm that occurred on June 29, 2012, in Northern Virginia, there were major failures of telecommunications services provided in Arlington County, Virginia, and in the region. The 911 services in Arlington, as provided by Verizon, failed due to the loss of backup power systems. The Verizon backup power generator failure signifies a lack of regulatory process to have either: 1) enforceable corporate testing requirements; or 2) independent and perhaps random checks of the

integrity of back-up power systems prescribed by the FCC or DHS. Beyond the failure of the 911 system, there was also a widespread failure of the telecommunications services on the Verizon FiOS fiber service because the backup batteries installed in consumer homes also failed well before their advertised capability of six hours of service. This would seem to imply either insufficient pre-installation testing of the batteries and/or installation of an inferior battery product in FiOS. Ramifications of this included a full shut down of residential telephone access to Arlington County government services.

Issues that appear to apply to all fiber networks in the U.S. would seem to include:

- Should there be national standards for back-up batteries, for alarms for failed batteries, and information kits for consumers, local governments and businesses as to phone outages during power outages as well as best practices to allow better reliability and sustainability of service?

- Should there be national standards related to wireless networks and maintenance of service during power outages, especially for networks used by governmental units and first responders? Would any such criteria be incorporated in FirstNet , the first responder network, currently in the planning phase?

- Is there a need for a public awareness campaign to inform the public (business and consumers) as to the various levels of vulnerabilities of fiber optic networks, coax and copper wire, and mobile cellular service? Indeed that even satellite telephone service will not sustain service unless there are power generators or vehicular charging systems available to recharge hand-held transceivers?

Power Supply: In emergency situations—whether natural disasters, industrial accidents or terrorist attack -- the lack of power can be a major liability with respect to timely and effective response and recovery. The new Community Energy Plan for Arlington has as one of its three major components the security and sustainability of its energy and power supply. It is believed that this is an element that deserves careful review at a national level as to whether district energy systems, solar, wind, geothermal or other power sources can be designed to provide emergency power backup during conventional electrical power plant outages. There is also concern about concentrations of ownership and power supply. We note that Dominion Power is a key supplier of electric and natural gas services in 15 states encompassing a vital supply of power to the national IT networks. Over-concentration of ownership and supply of power (for telecommunications and IT systems in particular) seems to be a legitimate concern for the FCC, National Telecommunications and Information Administration ("NTIA"), and DHS to consider in ensuring the sustainability of national communications and Internet services.

Assured power supply and rapid recovery should become an on-going element of the new national energy plan. District energy power plants, solar cell, geothermal, wind turbine energy systems and other design elements should be consistently reviewed as to their ability to supplement and support the survivability and sustainability of critical national infrastructure against emergency and attack conditions—as well as being particularly coordinated with regard to vital federal facilities located in Arlington, Virginia.

As noted above, periodic audits and associated action plans and assessments should be carried out in many areas related to vital telecom, IT, and power-related services. These assessments would address business and local governmental continuity/redundancy, threat detection/prevention, and end-user community readiness. These, in our view, should be reviewed annually in areas where there is critical infrastructure such as the Pentagon, large federal installations, the nation's largest airports, etc.

Telephone/Data Denial of Service (TDoS/DDoS): One of the recent areas of concern for telecommunications and IT reliability and sustainability comes from systematic attacks that can result from "capture" of a telecommunications pipe and can overload key emergency or vital governmental telecommunications networks. This type of attack can be mounted by those seeking to extort money from small or large businesses, to undertake a terrorist attack, or to disable 911 emergency communications networks. Also, in emergency conditions, public wired and wireless communications call failure rates increase dramatically due to call volume issues which strain telecom resources. Although Arlington County is exploring firewall protection so that its phone network could not be captured by nefarious or emergency TDoS/DDoS attacks, we believe that national telecommunications carriers and network providers should bear some regulatory burden to protect against the use of their networks for such TDoS attacks.

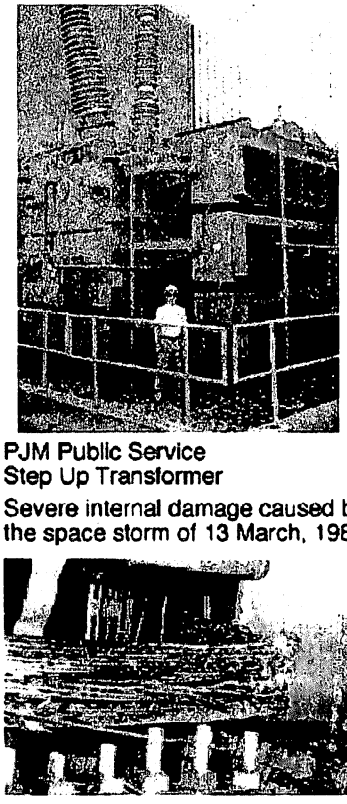
For an added cost, telecommunications providers currently have the ability to eliminate DDoS and perhaps TDoS attacks, as well as emergency demands through enhanced network management. However, as part of communications services to critical infrastructure providers such as public safety, energy, Internet, etc., the carriers should include such protections as part of any 911 and Internet data circuit related service. The burden of protecting the public good, health and welfare should not fall entirely upon the targets of these attacks, e.g. government facilities, data centers, energy providers, etc. Such carrier product integrity (protections) should include working with the potential critical infrastructure targets to manage and eliminate the unwanted traffic by using methods such as Border Gateway Protocols (BGP).

This is a vital public safety, life safety issue.

SCADA Protection: More and more cities, states and critical infrastructure related businesses are relying on Supervisory Control and Data Acquisition ("SCADA") systems for the control of traffic signals, routing of water and sewage systems, and control of power transformers and pipelines. Unfortunately, as these SCADA systems become more and more used and accessible, they are often not adequately protected against hackers or others that might use SCADA networks for terrorist attack. Better security standards, password protections, and security auditing procedures are needed. The same can also be said about switches in the nation's public switched telecommunications networks. In many cases, the access codes for PSTN switches are the same as when they were shipped from their supplier company. National standards and best practices should come from the FCC or DHS.

Coronal Mass Ejections and Solar Flares: In 1859, the so-called Carrington event that is today described by scientists as a coronal mass ejection (CME) occurred. The results of this event included telegraph

offices catching on fire, the aurora borealis being seen as far south as Cuba and Hawaii and a good deal of public concern. This event fortunately occurred well before the age of telecommunications, computers, the IT and electrical transformers. We have no idea what damage a similar event would inflict on the nation today, but the March 13, 1989, coronal mass ejection created damage and power outages in the Northeast and in Canada with a much less energetic solar storm. There are additional reasons to be concerned. NASA and ESA satellites have detected what appear to be emerging "cracks" in



PJM Public Service
Step Up Transformer
Severe internal damage caused by
the space storm of 13 March, 1989

Before and After Images of PJM Transformer Hit by March 1989 Solar Storm

(Graphic from J. Pelton, Orbital Debris and Other Hazards from Outer Space (2013) Springer Press, NY)

the Earth's magnetosphere. Recent studies concerning the Earth's periodic polar system (predicted to be about every 66,000 years) suggest that during times of transition the world's magnetic field might be reduced to only 5% of its normal level. We have no clear idea of how such cracks in the Earth's magnetosphere will affect the Van Allen Belts that afford us protection against solar weather hitting with maximum force. It is possible that we may be entering a period where coronal mass ejections and increased ultra-violet radiation might threaten electrical transformers and processors, electrical devices, telecommunications systems and IT networks with potentially devastating effects. It would appear prudent for the FCC and the DHS to seek from the National Science Foundation, NASA, and the National Academy of Scientists and Engineers an in-depth study of these phenomena and their potential for massive damage to the nation's telecommunications and IT networks and any protective or mitigating strategies that might be undertaken to lessen the deleterious effects of solar storms, especially if shifting conditions in the world's magnetosphere might serve to make us more vulnerable.

These comments reflect the efforts of the Arlington County Emergency Preparedness Advisory Commission, Arlington, ITAC, as well as information from the Arlington County Department of Technology Services, and the Arlington County Office of Emergency Management, to research major concerns related to emergency communications services and threats to the sustainability of telecommunications and IT services not only in our immediate jurisdiction but national threats as well.

Respectfully submitted,

ARLINGTON COUNTY INFORMATION
TECHNOLOGY ADVISORY COMMISSION

By: Joseph N. Pelton FOR
Joseph N. Pelton, Chairman

May 7, 2013.